The role of space in the security and defence policy of Turkey. A change in outlook: Security in space versus security from space

Ercan, C. and Kale, I.

The Role of Space in the Security and Defence Policy of Turkey
A Change in Outlook*: Security in Space* versus *Security from Space*

Abstract

Space and security domains are strongly related with each other. Nowadays, space is an indispensable part of security and defence policy, and it is increasingly becoming a critical infrastructure for strategic Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems. However, space is vulnerable itself to the new space threats. This study reviews the current and near future space role in Turkey's security and defence policy and aims to address the threats against space based capabilities. To provide security from space, space based systems shall themselves need to be secure in space to warrant the security. The concept of security from space starts with space security, in other words the security in space. This paper also highlights the emerging technological opportunities for these space threats to be secure in space in order to provide the security from space. According to the relevant taxonomy, a categorized opportunity proposal for more robust and resilient space/satellite projects' architecture is proposed for Turkey.

1. Introduction

Space technology, including satellites, is a proficient tool for both governments but sadly for terrorist organizations too in different perspectives. Governments have used technology to try and prevent terrorism and to ensure security, while terrorist-organizations take advantage of space to act freely. In this study, the potential threats against Space Based Applications (SBA) are categorized with their sources and their technological solutions are addressed mostly for defence space missions. Though most of the solutions are also valid for the commercial space segment, they are beyond of the scope of this study and will not be looked at in this paper.

Today's applicable threats and potential risks to missions from space have recently changed a lot in every aspect. Hence, the policy of security and defence needs to be reshaped accordingly. New forms of modern technology should also be applied wisely to mitigate and stop these threats. At this point, security applications based in space have many versatile capabilities to support real-time security and defence requirements.

Colarik [1] advises initially to understand the way of terrorist organizations before trying to be prevented from them. Real-time information supplied by recent space technologies is one of the most important pillars of their effective attacks. "Through utilization of the global information infrastructure and its underlying technologies, terrorists can operate in a virtual electronic world that provides them with numerous advantages for communication and coordination efforts, as well as assisting in their ongoing development and expansion efforts" [1].

SBA can be an ideal candidate for these important security needs and broader defence concepts. The reason for this continually increased demand for SBA is explained by Evans [2] as "partly to increased communication requirements in the face of enemy threats and partly due to increasingly sophisticated end-user requirements". For the time sensitive requirements, space originated data can contribute to *ensure security*. This paper explains both *the role of*

applications from space for security and defence and *the security in space*. It concludes that *security in space* is the first and utmost important step of providing *security from space*.

2. The Vital Need for Space for Improved Security and Defence Policy: Security from Space

Today, we live in a new space era and space is becoming more competitive and useful than ever before. Effective and efficient use of space and satellites is a power and a force multiplier for governments [3]. It is therefore clear that a proactive method, instead of old outdated approaches, will help to provide better and wider security, especially after the spread of global terrorism.

Fighting against terrorism is just one of the crucial rapid-response service dependents of the space sector. In this context, global space dependencies are detailed by NATO in [4] under following main five headings:

1. Positioning, Timing, Navigation (PTN) and Velocity
2. Intelligence Surveillance and Reconnaissance (ISR)
3. Integrated Tactical Warning and Threat Assessment
4. Satellite Communications (SATCOM)
5. Environmental Monitoring.

Precise and real-time confirmed information to decision makers/fighters on the field, whenever and wherever needed, provides an important information superiority and integrity capability in their security and defence strategy. It is generally believed that more Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems technology leads to information superiority [5]. Space can offer short notice high capacity services to anywhere at any time on Earth. To meet the required operational expectations for security and defence, finite SBA resources are required to gain the benefits of today's space technology.

Likely for NATO, in-orbit SBA are invaluable tools for Turkey's security and defence strategies too. Missile defence systems, satellite communication, and meteorological data provided from space are desperately needed by the decision makers to be able to see the risks/vulnerabilities and to predict the following stages of defence and security. Furthermore, PTN and ISR capabilities are required by staff to be aware of ongoing situation, organize the operational environment, foresee the future developments and propose to act harmoniously.

SBA are indispensable tool not only before and during but also even after the missions for the security and defence organizations. ISR data, mostly offered by reconnaissance satellites, is used in the decision process and served both to the fighters and to the commanders in near-real-time through Satellite Communications (SATCOM). For the planning of units, their deployment, tracking the blue force movements safely; precision and timely navigation, weather and ISR data of the Area of Responsibility (AOR) must be supplied to the commanders, staffs and the operation planners in a timely manner. The continuity and the sustainability of these time sensitive data updates are crucial because the gathering, enabling, employing, updating and serving process of these space originated weather, enemy and battlefield data continue simultaneously until the last minute of the mission and even after the operation. During the damage assessments or rescue operations, ISR data with infrared images from the AOR are helpful while locations are transmitted to the control stations almost instantly by Global Navigation Satellite System (GNSS) rescue signals in emergency situations.

At the same time, early warning for missile defences supports to active and passive missile defence for operational forces in the AOR and Area of Interest (AOI). SATCOM provides Command and Control (C2) of the Unmanned Aerial Vehicles (UAV) at Beyond Line of Sight (BLOS), communication on the move with the deployed and mobile forces and assets, and

reach-back link to the anchor stations/headquarters during these operations. SATCOM on the move offered by communication satellites and real-time useful secure information sharing provided by space based ISR assets give great advantage for defence and security organizations.

PTN will also be another critical asset during the whole mission. GNSS signals are widely used for positioning and navigation throughout operations. Additionally, synchronization of C4ISR systems as well as strategic defence missile systems use GNSS timing information. On the other hand, using GNSS satellites is required but not enough for time sensitive operations. Kaplan and Hegarty [6] discussed that "a single SPS GPS user can often attain better than 10m, 95% positioning and 20-ns, 95% timing accuracy worldwide. There are many applications, however, that demand levels of accuracy, integrity, availability, and continuity beyond even what a GPS PPS receiver can deliver." Continuously real-time updated data through GNSS, missile defence, ISR, and communication satellites is one of the most critical and important inputs for the decision makers, commanders, staffs, analysers and the fighters during all of the mission stages.

The combination of space based C4ISR assets and airborne assets is one of the requirements for commanders' critical information requirements and successful intelligence assessments. During all phases, most of the gathered and processed information is disseminated via SATCOM to wherever it is needed. Moreover, time-sensitive reports and orders are securely transferred through secure satellite links provided by hardened space segments.

On the other hand, meteorological data is another important input for scheduling SATCOM. Furthermore, it is critical to decide the most appropriate kind of space assets, such as planning either SAR satellite or EO satellite; as the former is not restricted by clouds. Space based ISR assets support to find and fix the adversaries' actions, their communication networks and their intention. They also provide the enemy's space based capability vulnerabilities in the context of AOR, AOI, space situational awareness (SSA) and sensitive infrastructures. Besides, borders are also monitored by space related capabilities. Space based assets provide not only mission critical security data for fighters but also situational awareness information for their own security in their orbits in space.

Friendly (blue) force tracking systems use GNSS data and SATCOM to transmit their own positions and receiving blue force positions for the situational awareness. The SBA's support in crisis continues through all stages of the operations. GNSS systems are also a tool for identifying the location of the enemy's jammer(s) and suggesting an alternative way for navigation as well as being vital for targeting.

Space derived data may be critical in re-evaluating the situations, re-configuring the plans and allocating of the units' resources, reserves and systems in near-real-time. For instance, under any jamming conditions that cannot be mitigated, non-GNSS guided systems may be an alternative to be considered. Likewise, under jamming conditions; more resilient EHF Band, STANAG 4606 Ed.3 X Band frequency hopping modems with tactical SATCOM terminals, other frequency band SATCOM terminals or narrowband UHF terminals may be alternatives for secure and robust communications.

As discussed above, growing numbers of security operations rely on space. The position in Turkey's Security and Defence Policy is not an exception. Dede and Akçay [7] depict Turkey's increasing space programmes in their study. The number of big space projects including low, medium and geostationary satellites [7] proves Turkey's dependencies on space for security and defence needs. Since 1996 when the first Türksat 1B satellite was launched, Turkey's PTN, C4ISR, SATCOM and monitoring assets have increasingly become more dependent on satellites. Turkey's satellite project roadmap (figure-3.11 in [8]) also accentuates the necessity of securing Turkey's SBA in space.

3. Turkish Space Programme Capabilities

Space-borne data from the satellites has been an essential and indispensable part of the security and defence cycle. Data for weather, command and control, communications, position navigation and timing, intelligence surveillance and reconnaissance, mapping, and early warning are mostly served by and through space based assets [4][9]. However, the increasing reliance on space is also turning to vulnerability. Having many SBA to provide security from space is not sufficient. To secure the space-originated data, satellites and space-based applications shall themselves need to be safe at first.

Now, broadened SBA is not a choice but it is a must for most governments in order to be able to consider and maintain global security and defence. As the kind of threats have dramatically changed recently, re-thinking the conceptual methods in attempt to keep pace with them, todays available space technology is an urgent and inevitable necessity for global security.

As mentioned earlier, like many other countries, Turkey is heavily reliant on space for its security and defence requirements. Space related technology has taken its place in the Turkey's strategic agenda for the last 40 years to be a regional player in the space arena [10–13]. For the past 10 years, Turkey's national space programs were accelerated at a remarkable pace. At present, Turkey is [13–15]:

- One of the 30 countries who have and operate their own LEO and GEO satellite/s in orbit/s,
- One of the seven NATO nations who have their own military X Band SATCOM payloads,
- The only other country, after France, that has developed national STANAG 4606 compatible X Band frequency hopping SATCOM modems,
- One of the two NATO countries who have successfully initiated and completed processed EHF R&D project,
- One of the several countries who have their own class 100,000 Assembly, Integration and Test (AIT) centre.

Satellite systems mainly have three orbits which have their own unique purpose with their specific advantage over the other one [16]: Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary/geosynchronous Earth Orbit (GEO). LEO satellites are generally used for earth observation and Intelligence, Surveillance, and Reconnaissance (ISR) purposes. In this respect for dual use, Turkey has the Bilsat, Rasat, Göktürk-1, Göktürk-2 and Göktürk-3 satellite projects [17–20]. For Global Navigation Satellite System (GNSS), MEO satellites are generally used for positioning and navigation purposes. Turkey has a Regional Positioning and Timing System (RPTS) Satellites project [21] and TUSAGA-Aktif project [22] as its augmentation system. Lastly, communication satellites commonly serve in GEO orbits in which the speed of the satellites is the same as that of the earth. Turkey has the Türksat 3A, 4A and 4B satellites in their orbits and has been developing its own intrinsic communication satellite (Türksat 6A) which is planned for launch in 2019 [23]. Turkey's Space Launch System Project is in its second phase and was been started in 2013 [24]. Turkey has many ongoing space related R&D projects for its operational requirements. Table-1 reflects the importance of space for Turkey in the context of security and defence policy.

Table-1: Turkey's Major Space Projects [17–27]

Orbit / Purpose	Turkey's Major Satellite/Space Projects
LEO Satellites / Earth Observation, Remote Sensing, Surveillance and Reconnaissance	Bilsat, Rasat, Göktürk-1, Göktürk-2 and Göktürk-3
MEO Satellites / GNSS	Regional Positioning and Timing System Satellites
GEO Satellites / Communication	Türksat 3A, 4A, 4B and 6A
Space Launch Systems	Space Launch System Project
Augmentation Systems / GNSS Augmentation	TUSAGA-Aktif

With the latest space and satellite technology achievements, Security and Defence Policy (SDP) cannot be effectively managed without space and satellite sourced data, information, systems, and services. Today Turkey's SDP, like many other developing and developed countries, is heavily dependent on space as highlighted in Table-1. Without SBA, the following actions cannot be accomplished easily in all AOR:

- Near-real-time C4ISR information is not viable and available to users wherever and whenever needed.
- The end users might have objection on the authentication of the provided information, questioning its integrity and reliability.
- The whole AOR cannot be observable and globally reachable.
- C4ISR cannot be provided if alternative terrestrial links are poor or missing.
- Setting up, initializing, operating and reconfiguration of the C4ISR will be time consuming which is very important factor in the AOR.
- Operational plans are done in a blind as a bat fashion.
- The continuous navigation and communication for the deployed, transportable and mobile headquarters/units will not be timely and correctly supportable.
- Identification friend or foe cannot not be achievable and the distinguishing them may be difficult to determine.
- Movements and logistics of friendly units cannot be effectively planned and tracked.
- Situational awareness including the neutral or foe units' movements cannot be accomplished.
- There will be a significant gap in the generating and understanding of a Common Operational Picture (COP).
- GNSS guided modern weapons and warning systems will not be controllable and manageable.
- After operations, battle damage assessment may not be provided.
- UAVs cannot be operational at BLOS.
- LEO and MEO satellites cannot be steerable at BLOS.

Therefore, space based security must be provided by a secured SBA to guarantee safety, integrity and operational success.

4. Space Threats that Turkey Needs to Take Into Account

There are many SBA for civilian and defence purposes through space based assets. Utilization of space for defence and security purposes is globally broadened and accelerated. It is reported in [28] that "Space, a domain that no nation owns but on which all rely, is becoming increasingly congested, contested, and competitive." Nevertheless, since satellites broadcast

over a vast area within their huge coverage maps, a signal from space make C4ISR systems more prone to threats from security point of view.

Satellites experience many threats in or from space, either intentionally or unintentionally. At the conceptual level, threats create risks, and risks generate the vulnerabilities of the SBA. Threat is described as “a potential violation of security” ([29] referred by [30]) while vulnerability is described as “weakness in an information system, cryptographic system, or components that could be exploited to violate system security policy and result in a security breach” [31]. The terms “risk” and “threat” are usually misused. Risk is commonly and wrongly referred to as threat. National Information Assurance glossary [32] defines the former as “possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability” and the difference between these two terms are formulated as “Threat=Capability×Intend” and “Risk=Probability×Harm”. This study mainly focuses on the threats excluding risks and risk assessment.

Threat sources can be man-made (generally termed threats), natural (generally called hazards) or caused by other factors. Although there is no common taxonomy of the threats to space [2], [30], [33-35], these threats are categorized and depicted as shown in Table-2.

Table-2: Threat Sources [2], [30], [33], [34], [35]

<table>
<tr><td rowspan="3">Targets (applicable to)</td><td colspan="3">Human-made Threats (Active or Passive)</td><td rowspan="3">Natural Hazards</td><td rowspan="3">Other Factors</td></tr>
<tr><td colspan="2">Intentional</td><td rowspan="2">Unintentional</td></tr>
<tr><td>Unique to each segment</td><td>Common for 3 segments</td></tr>
<tr><td>Space Segment</td><td>• Physical/Nuclear attacks on space segment
- Laser weapons, Laser blinding
- Guided munitions
- Deployed munitions
- Contamination
- High energy attack
- HANE (High Attitude Nuclear Explosions), Exo-atmospheric nuclear burst
- Scintillation, Atomic particles, High energy photons
- EMP, Blast
• Other satellites
• Debris (intentionally)
• Charged/Neutral particle beams</td><td rowspan="3">• Changing the environment on purpose
• Electronic Attacks (RF)
- RF weapons
- Jammers (interference, uplink and downlink jammers)
- High energy RF damage systems
- Burnout
• Cyber Attacks (non RF)
- Signal Interception, conversion, detection (direction findings, user location, traffic analysis, mission tipoffs)
- Spoofers (including fake telemetry and telecommand), Unauthorized commanding, Hacking, Hijacking
- Playback attack
- Eavesdropping
- Data exploitation
- Malware
- Supply chain infiltration
• Kinetic energy weapons</td><td>• Debris (unintentionally)
• Poor design and installations
• User/Operator errors
• Interference (unintentionally)
• Late or tainted delivery</td><td>• Orbital threats
- Space debris
- Near Earth objects</td><td rowspan="4">• International Laws and rules
• International Telecommunication Union and other space related organizations' rules
• International cooperation
• National priorities and caveats
• Economic factors and budget considerations
• Export Procedures
• Social factors
• Political factors
• Frequency allocation competition</td></tr>
<tr><td>Communication Link</td><td>• Multipath (intentionally)</td><td>• Multipath (unintentionally)
• Interference (unintentionally)</td><td>• Natural Earth catastrophes
• Space Environment
- Space weather
- Meteor Showers/storms
• Solar activities
- Radiation
- Geomagnetic storms,
- Ionospheric Scintillation
- Solar flares
- Cosmic Rays
- Coronal Mass Ejection
• Multipath</td></tr>
<tr><td>Ground Segment (including launch facility)</td><td>• Physical Attack on control stations and launch facilities
• Takeover, Distruption, Destruction</td><td>• Interference (unintentionally)
• Late or tainted delivery
• Launch failures</td><td>• Natural Events (Earthquake, flooding, etc.)
• Solar activities
- Radiation
- Geomagnetic storms,
- Ionospheric Scintillation
- Solar flares
- Cosmic Rays
- Coronal Mass Ejection</td></tr>
</table>

In generally, satellite systems consist of three segments [36]: The space segment, communication link, and the ground segment (including users and launchers). In this study, space threats were considered for all parts of the system including the ground segment, space segment, communication link and the launching site. In Table-2, threats against each of these segments were categorized according to their applicable targets. Threat sources were also classified according to their origins that can be either man-made, natural, or arisen from other reasons for each applicable segment. As seen from the Table-2, there are many both intentional and unintentional space threats that must be considered in costly space/satellite projects.

Today, we witness numerous threats and vulnerability examples globally. Hreha et al [37] provide evidence for sufficient real jammed examples of satellite communications to justify the evidence. Kendall [38] boasts that "there is a growing concern that threats against vital space capabilities may increase during the next decade as a result of both natural and man-made hazards and the possible development of disruptive and destructive counter-space capabilities". It is most likely that intentional threats and damage to satellites may be a reason for a wars in future.

Readers are referred to [39–43] for further threat news. The worst debris problem exists in LEO orbit. The Turkish Air Force had to make Göktürk-2's third collision avoidance manoeuvre on 27 April 2016 because of space debris caused by China's Fengyun-1C DEB[44].

Space-borne systems are increasingly subject to the aforementioned man-made threats on a daily basis, which require additional countermeasures. Moreover, a space natural environment is in itself a hazard for satellites. SBA are becoming more and more vulnerable to these hazards and threats. As today's threats are very different from the past, it is for sure that the threats against space will exist, and the threats and their countermeasures in the future will be different from today's. It must be kept in the mind that these measures will add both design complexity and cost, and may decrease the communication throughput availability. The following section describes possible ways of securing the SBA which are also valid for Turkey.

5. Technological Opportunities for Space Threats

In the 21st century, more nations realized that satellites are the key enabler systems for their security and defence policies. Vulnerabilities in space, due to aforementioned threats, may have detrimental effects on these two important areas. Their uniqueness of providing huge coverage areas make satellites an indispensable part of communication and information systems. However, unfortunately, this is also a disadvantage for satellites since their links are visible and trackable from all around the world and the earth's surface, and can be subjected to threats easily.

It is necessary for defence/military satellites to provide services and to continue to communicate 24/7 under threats. Solin [45] discusses the LEO satellite vulnerabilities and warns that "…one 20 kT nuclear weapon exploded at the right altitude above the Earth, would cause all **unhardened** LEO satellites to die in hours, days, or weeks. Less appreciated is that LOS X-rays and neutrons from a high-altitude nuclear burst, can also damage or upset **unhardened** GEO satellites" [45].

Therefore, security in space is seen as a vital necessity, especially for defence/military satellites. The previous sections in this paper covered the current threats to space. There are many emerging techniques to secure the SBA from these threats. Since the protection measures are very costly, protection levels are set according to the user requirements. Although the space segment is the main focus of this paper, the entire infrastructure including the space segment, ground segment, communication link and launch facility are taken into account too.

The uniqueness of defence/military satellites demand protected, robust and survivable services and requires them to withstand the threats in all conditions. There are many space-related taxonomy studies for space mission assurance in the open literature. We follow the guidance in [35] since it sets the opportunity to analyse the conceptual framework sufficiently with the right number of classifications.

This paper is developed around this taxonomy in which space mission assurance has three interrelated basic conceptual domains: *1. Defensive operations, 2. Reconstitution and 3. Resilience* [35]. To address most of the threats against space (see Table-2) in space-dependent operations [4], widely known resilience domain shall be considered with the other two critical components of the space mission assurance, which are defensive operations and reconstitution, since they may also be very harmful to space systems. The defensive operations domain includes off-board protection methods while on-board protection methods are discussed in the resilience domains [35].

In this paper the following framework of methods and strategic vision is proposed for Turkey's future resilient and robust SBA (see Table-1) to secure the safety in space. To supply the requirements of Turkey's security and defence policy and to provide SBA's safety, possible solutions are proposed for each domain sequentially.

5.1. *Defensive operations* are the self-protective actions that disrupt the attacker from harming space systems or offering forewarnings before their intention [35]. This capability requires awareness of the intentional or unintentional threats and needs manoeuvring of the SBA accordingly. For example, Turkey made its third collision avoidance manoeuvre on 27 April 2016 to avoid to collision with space debris caused by China's FENGYUN-1C DEB for its national reconnaissance satellite Göktürk-2 [44]. These coordinated and systematic manoeuvres of SBA by Turkish operators with the provided situational awareness warnings by itself or friendly capabilities are of primary importance for Turkey to operate SBA securely. On the other hand, on-board self space situational awareness, threat detection systems, restore capabilities and mitigation procedures including software capabilities after threats/hazards capabilities may be good defensive space operations for Turkey. Disaster recovery plans, interference mitigation plans, personnel security clearances, and Concept of Operations (CONOPS) are other defensive operations that need to be ready and operational in space.

5.2. *Reconstitution* is "the plans or operations to bring new assets on line in order to replenish lost or diminished functions to an acceptable level for a particular mission, operation, or contingency after an attack or catastrophic event" [35].

Turkey initiated Göktürk-1, Göktürk-2 (now in-orbit) and Göktürk-3 LEO satellite projects for the Turkish Armed Forces' (TAF) reconnaissance and surveillance requirements [17-20]. Turkey's other important space program is the Regional Positioning and Timing System (RPTS) (known in Turkish as "Bölgesel Konumlama ve Zamanlama Sistemi-BKZS") project to provide positioning and timing information to the TAF in the area of interest at all times [21]. On the other hand, the Türksat series Türksat 3A, Türksat 4A and Türksat 4B satellites are serving in their GEO orbits for communication purposes [25]. Additionally, the Türksat 6A satellite project including space and ground segments was signed on 15 December 2014 [23] and two more, Türksat 5A and 5B, satellite projects are currently being planned [46].

For the reconstitution measures, Turkey may consider to launch new Türksat, Göktürk and RPTS satellites for back-up operational capability. Moreover, additional communication and C2 ground segments should be established for LEO (Göktürk), MEO (RPTS) and GEO (Türksat or milsatcom) satellites. More C2 ground segment is especially important for the LEO Göktürk satellites to benefit and maximize the naturally limited download times and to be able to send the mission orders to the satellite anytime. Deployable/transportable/mobile backbones and

ground stations may help reconstitution quickly. Though, Turkey has an Assembly, Integration and Test (AIT) centre for space systems, a second AIT may serve Turkey advantageously to be able to build more satellites simultaneously whenever needed.

Enlarging the launch sites in Turkey's Space Launch System Project will provide reconstruction and provide sustainability of the Turkish satellite roadmap independently [24]. On the other hand, both further guaranteed frequency bands allocated by the International Telecommunication Union/NATO and supplementary signals will boost Turkey's capacity through extra links. Reconstitution domain is not sufficient by itself but it is complementary for defensive operation and resilience domains.

5.3. USA DoD [47] defines the third domain which is *Resilience* as "the ability of an architecture to support the functions necessary for mission success with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats, in spite of hostile action or adverse conditions". There are many ways to address the known threats to space and make SBA more resilient. Although most of the threats and countermeasures are classified in the "protection" subtitle, there are five more different aspects of having resilient space assets. Resilience has six common sub-elements formulated as: Disaggregation, Distribution, Diversification, Deception, Protection and Proliferation (D^4P^2) [47]. These sub-elements are explained and their application methods are proposed for Turkey in the following parts of the paper.

5.3.1. *Disaggregation* of the space capability is to have different kinds of capabilities on distinct payloads or different satellites [35]. One way of dealing with the increasing threat to space is to separate the payloads and to differentiate the satellites according to the wideband/narrowband, protected/unprotected and core/extended operational necessities. The operational space requirements shall be classified into tactical, operational and strategic requirements. For strategic communications, protected satellites may be allocated. While protected core services for strategic communications may be provided through military satellites or military payloads [15], operational or tactical extended communications may co-exist with commercial Türksat satellites or hosted payloads on other *allied or friendly* satellites. For social satellite communication requirements, non-protected commercial Türksat satellites (Ku band) may continue to be used.

Different frequency bands (X, Ku, Ka, military Ka, UHF and EHF) for different needs are example of disaggregation to productize Turkey's space and SATCOM capabilities. Turkey may have separate EHF satellites [15] for its strategic protected wideband satcom needs. Separate UHF satellites [15] may be used for narrowband satcom requirements of tactical users. Different X band payload on different satellite may serve to operational level users. As a conclusion, it is wise to plan different X (7250-7750 MHz, 7900-8400 MHz), Ku (12-18 GHz), Ka (20.1-21.2 GHz, 30-31 GHz), UHF (240-270 MHz, 290-320 MHz) and EHF (43.5-45.5 GHz) band capacities by disaggregating them on different payloads and on different satellites for Turkey, instead of having all bands on a single satellite.

Turkey's first internally designed high resolution LEO satellite, Göktürk-2, has an Electro-Optical payload. On the other hand, Turkey is on the right path by initiating a different satellite to provide high-resolution images in any weather condition for a different requirement [20] by signing an additional Göktürk-3 Synthetic Aperture Radar satellite project for different strategic requirements.

Turkey, as an emerging space country, will benefit from disaggregation of the space and satellite capability on different platforms in three ways: It will minimize the space system design complexity, alleviate and share the risks, and increase its space readiness.

5.3.2. *Distribution* is the design of the system operating as a centralized node of nodes which are performing together for the same mission [35]. RPTS is a good implementation example of SBA distribution for Turkey. To address the regional timing and navigation system requirement, the RPTS should be a distributed system. Distributed design of the RPTS project will prevent the single point of failure from being an issue, avoid being a single and an easy target to threats, and increase the survivability of the GNSS system. Another distribution way of Turkey's space capability may be to have on-board X and Ku band cross-link designs to transition between different bands to extend the coverage area of each different band. Small satellite concept is another means of distribution of the space systems which may allow Turkey to reach space in a relatively cheap manner.

5.3.3. Diversification is the concept of having the separate platforms/orbits/systems and/or using civilian, commercial or international partners' space capacities for a particular mission [35]. Like other nations, X band space capacity is the core and an indispensable operational satellite communication requirement for Turkey. Turkey has X band capacities on different satellites [15]. Following X Band payloads should not only be on different satellites but also these satellites should be in alternative orbits. Additionally, for the X band requirement, civilian or commercial X band opportunities may be alternatives when the demand is unexpectedly increased. Alternatively, NATO, EU, NATO/EU members, and friendly or allied nations are other partner choices. Turkey can use their X band space capability wherever the operational need is not in the Türksat satellites' coverage area.

Inter-satellite Link Systems (ISL) is another diversification method for Turkey to consider to have links between LEO Göktürk satellites and GEO Türksat satellites to maximize the downlink and uplink capacity and extend the coverage areas.

Commercial satellite communications (comsatcom) instead of military satellite communications (milsatcom), hosted payloads and international partners are also other ways of diversification for further resilient space needs. Additional satellite communication requirements in Ku, Ka, military Ka, UHF, EHF bands and combination of them may be supplied in a similar way. As another MEO example, Glonass, GPS or Galileo space segments via international collaborations can be used for the PTN services with the RPTS project. On the other hand, other LEO satellites (of partners or commercial) can be alternative systems for Turkey's ISR requirements to achieve the same mission goal. By diversifying the space capabilities on different satellites, in additional orbits or by different systems, Turkey will be able to use alternative means of risk sharing, cost reduction and greater collaboration in space.

5.3.4. *Deception* is the action of misleading others about one's real strengths and weakness in space capability [35].Turkey should have critical space technology including design, software, integration, testing and launch know-how. Adversaries will not be able to decide where the centre of gravity is and will hesitate to attack if they don't know about the actual operational capacity. By building space capacity domestically, it will be easier not only to hide one's design constraints, limitations, strengths or operational vulnerabilities but also to keep the intention and the operational capability secret. Deception will also decrease the possibility of being a target, provide strategic surprise on enemies [35], and increase the survivability.

5.3.5. *Proliferation* is the act of enlarging the number of the same platforms, payloads or system capabilities for the unique mission [35]. L, C, Ku and Ka bands are the applications of commercial satellites while UHF, X, military Ka and EHF are generally the examples of military payloads for communication satellites. Military satellites serve protected or unprotected and narrowband or wideband communications.

Turkey has X and Ku band capacities [15] for the current satcom needs from Europe to Asia and North Africa [25]. Ku band is used for social needs generally and X band is mainly used for military communications by the TAF. However, the number of existing X and Ku band payloads may be increased for upcoming requirements especially after UAVs are operationally used. Since the space/satellite projects and their frequency coordination are long-running procedures and satellites take a long time to be build, expected and unexpected upcoming operational needs shall be considered at least seven years before launch.

Additionally, more payloads and satellites to provide the communication requirements in Ka, military Ka, UHF and EHF bands may be planned for future needs or increased throughput. Similarly, increasing the number of RPTS/Göktürk satellites, the number of downlink of Göktürk satellites, and the number of ground facilities for space-based services will help Turkey to proliferate its space capability. Additional national and international infrastructures will extend the communication links which will intensify the real-time communication and information sharing. The number of each similar LEO, MEO, and GEO satellites will increase as a result of the proliferation, thus the availability and the reliability of Turkey's space systems will be boosted.

Sub-system or equipment level redundancy and payload level redundancy also provides and furnishes Turkey's space proliferation. On the other hand, improving the TAF's TAFICS (Turkish Armed Forces Integrated Communications System) [15] terrestrial fibre optic link, Radio Link systems and linking hot/cold redundant ground control stations via the TAFICS network will satisfy proliferation and enhance the resilience.

5.3.6. *Protection* is the active and passive actions taken to continue to perform the mission 24/7 in all situations [35] including harsh conditions. Since, satellites generally serve at least seven (LEO satellites) to fifteen (GEO satellites) years in their orbits, Turkey should take space threats into considerations starting from their initial plan, and design them accordingly. Because, there will be no chance to change the in-orbit spacecraft's design during their life time after launch.

The protection methods which may be taken into consideration by Turkey especially for military/defence space projects are listed below. These methods include but are not limited to the following [2], [30],[33–35]:

- Anti-Jamming techniques including Antenna Nulling and Spread Spectrum
- Spread spectrum includes direct sequence and frequency hopping methods, and CDMA (for fading, jammers, spoofing, interception, cyber and nuclear attacks)
- Steerable antennas and steerable beams (to avoid jammer and to use whenever and wherever needed)
- Antenna handover
- Spot beams
- Limited coverage area instead of global coverage area (for some cases)
- Digitally programmable (software defined) satellites
- Scrambling and interleaving for low probability interception
- Dynamic rate management
- Adaptive coding
- Spontaneous adaptation methods to the stress
- On board processing for electronic attacks to satellites, interception, cyber and nuclear attacks
- Hosted internal decoys
- Nuclear hardening
- RF Limiter
- On demand manoeuvring capability of the satellites

- Inter-satellite links to mitigate physical attacks to satellites, interception, detection and cyber-attacks
- Red and black distinction architecture
- National encryption (including telemetry, telecommand and space originated data)
- Authentication and identification of users against spoofing, adversary access, and interruptions to both space and ground segments.

For the common jamming conditions, using frequency hopping modems and hardened CDMA can be good applications for the mitigation of space threats. Turkey has produced its own NATO STANAG 4606 Ed.1 compatible frequency hopping modems [48]. In the presence of HANE, the use of EHF band may be necessary [2]. Turkey is the second NATO nation, after USA, who produced a *processed EHF engineering model* domestically [14,15] for this purpose. Turkey should extend this capability and have in-orbit processed EHF band for secure milsatcom need.

As a conclusion, the SBA shield requires more redundant and resilient hardware and software. Its protection will enable Turkey to continue to undertake its operations and duties continuously, securely, anytime, and anywhere in a reliable way. Thus, in the event of any threats, attacks or hazards Turkey will be able to restore its space systems immediately at the aftermath of threats or hazards. Moreover, it will increase self-awareness and robustness in space for Turkey. It is clear that protection against all possible threats adds considerable costs and may not be affordable [49], hence Turkey should also decide the appropriate degree of protection for different levels of user.

Disregarding and ignoring the threats against space missions may result in the loss of critical space/ground resources or unauthorized destruction of C4ISR systems. As a result, threats may affect the mission success and may make the entire mission impossible. All threats attempt to injure either the physical part of the space system or the communication link between the space and ground segment. Space mission planners should use aforementioned technologically available solutions whenever appropriate, carry out risk assessments and have a close coordination with the security experts.

SBA provide incomparable opportunities for the security and defence strategies with emerging technologies. Many space and satellite projects involve foreign players. To address requirements in Turkey's security and defence policies, a new more space oriented approach should be considered.

Today's complex and changing needs of security and defence requirements call for technology aided and driven methods to overcome the threats in time. SBA will provide better, deeper and all time security and defence. It seems that they will be widely used in the future too. The security in space issues influence international relations and the new global security thinking. Though it naturally has regional issues and differences, it unmistakably calls for international collaborations.

Being aware of other operational satellites, their capabilities and space debris are also important factors for the efficient use of satellites and space for security and defence purposes safely and efficiently, and in a sustainable way.

6. Result and Discussion

Space is a valuable means to Turkey for its security and defence needs. Satellites provide a major contribution to the security and defence sector with their advantages of flexible, cheaper, resilient and global coverage service capability. As the use of satellites and their capabilities continues to increase, they are also being intentionally targeted more than ever

before [40–44]. Not only the man-made threats but also space debris are increasingly becoming potential threats against satellites.

It is clear that both the demands and the threats for satellites and space programs are continuously increasing [40–44]. The most affected orbit is LEO since the debris are continuously getting worse and congested in this orbit. A single protection architecture will not be enough for all threats and hazards. Hence, international collaborations in space may provide better security in space for Turkey.

As space and security becomes increasingly global, threats force nations to cooperate more with each other. The EU and its strategically important partner, Turkey, should seek to meet the new security challenges and requirements together by a new security dimension coming from *space*, wherever possible, in an international collaboration. International/regional space cooperation and partnerships will address the vulnerabilities of the SBA and sustainability of the secure space utilization.

Satellites are game changers and they are needed for more rapid, more swift, more intelligent, more effective and more precise decisions and actions. Peacekeeping and humanitarian operations are all around the world. These operations need secure BLOS communication, more resilient space segments and better situational awareness for information integrity and superiority. The satellite is at the heart of the information integrity and superiority and the key to strategic plans, sovereignty and autonomy. Satellites need to be robust in harsh and Electronic Warfare (EW) environments. Hence, nuclear protection for satellites is urgently called for the fragile and uncertain future battlefield and operational AOR. Protected space and secured communication links are of great importance for successful operations.

Security and defence take the advantages of uniqueness of SBA, especially feature of wide coverage and near-real-time communications. Besides the aforementioned applications, numerous other security and defence requirements can extensively be met by the intrinsic achievements of space originated data. Global coverage, interoperability, robustness, cost efficiency, flexibility, multicast and broadcast communications, near-real-time communications, place and terrestrial infrastructure independence, reliability, high resolution images, quick connectivity, higher bandwidth, BLOS command and control of UAVs, minimized operation costs, rapid deployment of the ground systems and usability in hazardous as well as hostile environments are the main benefits of SBA. This paper has shown that these unique capabilities make satellites an indispensable tool for all nations' SDP including both Turkey's and EU's, but they are also vulnerable to space threats.

To defend against terrorism is one of the main legal duties of national security and defence authorities. Terrorism is not new and happens globally. In the year of 2016, there were many shocking attacks all around the world. Terrorists achieve their goals, *worldwide deep fear by attracting the awareness of the media*, by the help of the broadcast media who can serve and convey these kind of event news as they happen in real-time worldwide simultaneously via the use of technology often through the global coverage capabilities of satellite communications. Until more serious steps including technological perspectives are considered, the terrorist threats may not end, and they may occur again at anytime and anywhere including in space. Hence, secured space needs to be considered to ensure that security is secured.

Space assets are also key for modern communication and warfare. SBA are subject to the aforementioned man-made threats. Additionally, the natural environment of space is itself a hazard for satellites. SBA are becoming increasingly vulnerable to these hazards and threats. Changing requirements, diversified threats and growing hazards require new types of affordable secure approaches to match defence and security requirements and clearly without a doubt need additional countermeasures. As a result, one of the most important infrastructures, satellites, should be better protected for defence and governmental users. However,

consideration should be given to the emerging threats for all SBA and also to designing and using them accordingly.

Turkey should consider the aforementioned three-interdependent cross domain abilities at the conceptual level to secure its safety in the space-related architecture, design and evaluation processes which are essential to become a regional space power.

Acknowledgment:

This study was supported by funding from the Jean Monnet Scholarship Programme. The views in this article represent only those of the authors and do not represent the view of any organization, institution or government in any way or form.

References:

[1] A.M. Colarik, Cyber Terrorism - Political and Economic Implications, Igi Global, 2006. doi:10.1016/S1361-3723(01)01117-4.
[2] B.G. Evans, Satellite Communication Systems, IET, 1999.
[3] J.W. Canaday, Space Technology: Force Multiplier or False Sense of Security, 1994. http://www.dtic.mil/dtic/tr/fulltext/u2/a279726.pdf.
[4] NCIA NATO, D. Allen, P. Bartolomasi, R. Essad, T. Kreitmair, L. Patten, et al., Space Support to NATO Operations: NATO Dependencies on Space (Revised), No Single NATO Operation without Space, 2015.
[5] UK Ministry of Defence, Information Superiority Joint Doctrine Note 2/13, Dev. Concepts Doctrin. Cent. (2013). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/239342/20130813_JDN_2_13_Info_Super.pdf (accessed June 3, 2016).
[6] E.D. Kaplan, C. Hegarty, Understanding GPS:Principles and Applications, Second Ed., Artech House, 2006.
[7] G. Dede, M. Akcay, Technology foresight in practice: A proposal for Turkish space vision, Space Policy. 30 (2014) 226–230. doi:10.1016/j.spacepol.2014.07.002.
[8] G. Dede, Space Technologies Foresight Study for Turkey, Turkish Military Academy, 2013.
[9] A. Kolovos, Why Europe needs space as part of its security and defence policy, Space Policy. 18 (2002) 257–261. doi:10.1016/S0265-9646(02)00038-3.
[10] F. Ince, Possible Turkish Participation in Joint Euro-Med Space Projects, in: Recent Adv. Sp. Technol. 2003. RAST'03. Int. Conf. On. Proc., 2003: pp. 458–463.
[11] T. Ozalp, Space as a strategic vision for Turkey and its people, Space Policy. 25 (2009) 224–235. doi:10.1016/j.spacepol.2009.09.005.
[12] E. Solakoglu, B. Hassoy, Ieee, Space research programs in 21st century and challenges for Turkey, 2007 3rd Int. Conf. Recent Adv. Sp. Technol. Vols 1 2. (2007) 54–58. doi:10.1109/rast.2007.4284051.
[13] A.B. Uygur, O.O. Haktanir, F. Yilmaz, H.G. Isik, Z. Asansu, Turkey's New Assembly, Integration and Test (AIT) Center and Its Comparison with AIT Centers in Europe, in: In Recent Advances in Space Technologies (RAST), 2015 7th International Conference on, 2015: pp. 71–74.
[14] C. Ercan, C.. Barim, Turkish Military Satellite Communication-Today & Future, in: Glob. Mil. Satell. Commun. Conf., London, 2014.
[15] M.B. Usta, Muhabere Elektronik ve Bilgi Sistemlerinde Tarihsel Bir Yolculuk, Silahlı Kuvvetleri Derg. (2015) 423: 44–52. http://www.tsk.tr/Content/pdf/yayinlar/skd_423.pdf.
[16] T.M. Braun, Satellite Communications Payload and System: Focus on Satellite Payload, Wiley-Blackwell, 2012.

[17] SSM, Reconnaissance and Surveillance (GÖKTÜRK) Satellite, (n.d.). http://www.ssm.gov.tr/home/projects/Sayfalar/proje.aspx?projeID=53 (accessed March 23, 2016).
[18] TÜBİTAK, GÖKTÜRK-2 Uzayda Üçüncü Yılını Tamamladı, (2015). http://www.tubitak.gov.tr/tr/haber/gokturk-2-uzayda-ucuncu-yilini-tamamladi (accessed December 21, 2015).
[19] TÜBİTAK UZAY, GOKTURK-2, (2016). http://uzay.tubitak.gov.tr/en/uydu-uzay/gokturk-2 (accessed March 23, 2016).
[20] SSM, GÖKTÜRK-3 SAR Satellite System, (2016). http://www.ssm.gov.tr/home/projects/Sayfalar/proje.aspx?projeID=42 (accessed December 1, 2015).
[21] SSM, Regional Positioning and Timing System Project, (2013). http://www.ssm.gov.tr/home/projects/Sayfalar/proje.aspx?projeID=224 (accessed June 14, 2016).
[22] General Command of Mapping, Turkish National Permanent GPS Stations Network (TNPGN), (2016). http://www.hgk.msb.gov.tr/english/arama-sonucu?deger=TUSAGA (accessed June 14, 2016).
[23] TÜBİTAK UZAY, TURKSAT-6A, (2016). http://uzay.tubitak.gov.tr/en/projeler/turksat-6a (accessed January 15, 2016).
[24] SSM, Space Launch System Project, (2016). http://www.ssm.gov.tr/home/projects/Sayfalar/proje.aspx?projeID=222 (accessed December 1, 2015).
[25] Türksat, Türksat Satellite, (2016). https://www.turksat.com.tr/sites/default/files/uydu/turksat_satellite_services_and_solutions_2016.pdf (accessed March 16, 2016).
[26] Ö. Yıldırım, S. Bakıcı, Ç. Mekik, Tusaga-Aktif sisteminin Tapu ve Kadastro Müdürlügüne Katkıları, (n.d.). http://geomatik.beun.edu.tr/mekik/files/2012/12/HKMO-TUSAGA-AKT.pdf (accessed March 3, 2016).
[27] TÜBİTAK, TÜRKSAT 6A Projesi ön Tasarım Gözden Geçirme Toplantısı, (2016). http://www.tubitak.gov.tr/tr/haber/turksat-6a-projesi-on-tasarim-gozden-gecirme-toplantisi (accessed January 15, 2016).
[28] US DoD, National Security Space Strategy, (2011). https://fas.org/irp/eprint/nsss.pdf (accessed March 10, 2016).
[29] ISO, Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture, 1989.
[30] The Consultative Commitee for Space Data Systems, Security Threats Against Space Missions, CCSDS 350.1-G-2. (2015) 2–1. http://public.ccsds.org/publications/archive/350x1g2.pdf (accessed June 4, 2016).
[31] The Consultative Commitee for Space Data Systems, Information Security Glossary of Terms, CCSDS 350.8-G-1. (2012). http://public.ccsds.org/publications/archive/350x8g1.pdf (accessed June 3, 2016).
[32] I. Assurance, National Information Assurance (IA) glossary, Natl. Secur. Syst. Instr. (2010) 103. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf (accessed August 25, 2016).
[33] A. Proctor, GNSS Vulnerability, in: Sp. Innov. Congr., 2016.
[34] C. Dargeou, E. Boucharlat, Addressing the wide range of military communications, in: 17th Annu. Glob. MILSATCOM, London, 2015.
[35] Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, Space Domain Mission Assurance: A Resilience Taxonomy White Paper, (2015) 1–10.
[36] P. Misra, P. Enge, Global Positioning System Signals, Measurements, and Performance, Ganga-Jamuna Press, 2001.

[37] W. Hreha, D. Grybos, R. Singh, Commercial SATCOM communications protection: Commercial SATCOM resilience to jamming, Proc. - IEEE Mil. Commun. Conf. MILCOM. (2011) 2302–2306. doi:10.1109/MILCOM.2011.6127665.
[38] D. Kendall, International Collaboration for the Peaceful Uses of Outer Space, (2016).
[39] D.E. Denning, P.F. MacDoran, Location-based authentication: Grounding cyberspace for better security, Comput. Fraud Secur. 1996 (1996) 12–16. doi:10.1016/S1361-3723(97)82613-9.
[40] C. Arthur, Chinese hackers suspected of interfering with US satellites, Guard. (2011). https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected (accessed April 1, 2016).
[41] SpaceNews Editor, NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft, SpaceNews. (2006). http://spacenews.com/nro-confirms-chinese-laser-test-illuminated-us-spacecraft/ (accessed March 10, 2016).
[42] M. Gruss, Russian Satellite Maneuvers, Silence Worry Intelsat, SpaceNews. (2015). http://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/ (accessed February 3, 2016).
[43] L. David, Effects of Worst Satellite Breakups in History Still Felt Today, Space.com. (2013). http://www.space.com/19450-space-junk-worst-events-anniversaries.html (accessed April 17, 2016).
[44] Turkish Air Fiorce, Third Collision Avoidance Maneuver in Space, (2016). https://www.hvkk.tsk.tr/tr-tr/Havacılık_Köşesi/Özel_Siteler/Keşif_Uydu_Komutanlığı/Duyurular/ArtMID/532/ArticleID/517 (accessed May 27, 2016).
[45] J.R. Solin, Third world radiation threats to satellites, IEEE Trans. Aerosp. Electron. Syst. 42 (2006) 1437–1445. doi:10.1109/TAES.2006.314583.
[46] Türksat 5A ve 5B uyduları için geri sayım başladı, Milliyet. (2016). http://www.milliyet.com.tr/turksat-5a-ve-5b-uydulari-icin-ekonomi-2298823/ (accessed August 25, 2016).
[47] US Department of Defense, Space Policy, 3100.10. (2012) 12. http://www.dtic.mil/whs/directives/corres/pdf/310010p.pdf (accessed June 3, 2016).
[48] Undersecretariat For Defence Industries (SSM), SATCOM EPM (FREQUENCY HOPPING) Modem, Turkish Def. Ind. Prod. 2015-2016. (2016). http://www.ssm.gov.tr/home/tdi/Documents/ssmkatalog_en.pdf (accessed August 25, 2016).
[49] S. Marsh, W. Rees, The European Union in the Security of Europe: From Cold War to Terror War, Routledge, 2011.

Dr. Cihan ERCAN is a postdoctoral researcher at Applied DSP and VLSI Research Group at Faculty of Science and Technology at the University of Westminster. Dr. Ercan's research interests include satellite system, unmanned aerial systems, operations research and security systems. He received his first MSc. degree (2001) in Information Systems from Middle East Technical University, Ankara, Turkey, the second MA degree (2004) in Education Management and Assessment from Yüzüncü Yıl University, Van, Turkey, and the Ph.D. degree (2013) in Operations Research from Turkish Land Force Academy Defense Science Institute, Ankara, Turkey. He is the recipient of fellowships from TUBITAK and Jean Monnet Scholar Programs. He has been Turkish representative to NATO for NATO Satellite Communication Capability Team from 2004 to 2015 and has been inspired by many national and international experiences including C4ISR, satellites, communications, security, and UAV systems.

Prof. İzzet KALE received the BSc (Hons) degree Electric and Electronic Engineering from PCL, London, UK, the MSc. degree in the Design and Manufacture of Microelectronic Systems from Edinburgh University, Scotland, U.K., and the Ph.D. degree in Techniques for Reducing Digital Filter Complexity from the University of Westminster, London, U.K. He is currently Head of the Department of Engineering and Professor of applied DSP and VLSI systems, and Founder and the Director of the Applied DSP and VLSI Research Group at the University of Westminster. His research and teaching activities include digital and analog signal processing, silicon circuit and system design, digital filter design and implementation, and A/D and D/A sigma–delta converters. He is currently working on hybrid GNSS GPS/Galileo/Glonass/Compass receiver structures and systems that are resilient to interference and jamming.